

ON THE RANKS OF ELLIPTIC CURVES WITH ISOGENIES

HARRIS B. DANIELS AND HANNAH GOODWILLIE

ABSTRACT. In recent years, the question of whether the ranks of elliptic curves defined over \mathbb{Q} are unbounded has garnered much attention. One can create refined versions of this question by restricting one's attention to elliptic curves over \mathbb{Q} with a certain algebraic structure, e.g., with a rational point of a given order. In an attempt to gather data about such questions, we look for examples of elliptic curves over \mathbb{Q} with an n -isogeny and rank as large as possible. To do this, we use existing techniques due to Rogers, Rubin, Silverberg, and Nagao and develop a new technique (based on an observation made by Mazur) that is more computationally feasible when the naive heights of the elliptic curves are large.

1. INTRODUCTION

It is a fundamental theorem in arithmetic geometry that the rational points on an elliptic curve can be given the algebraic structure of a finitely generated abelian group. This was first proven by Mordell [15] in 1922 for elliptic curves over \mathbb{Q} and then vastly generalized by Weil [25], who proved in 1929 that the group of rational points on an abelian variety defined over a number field is finitely generated. Thus, if E/\mathbb{Q} is an elliptic curve, there exists an integer $r \geq 0$ and finite abelian group $E(\mathbb{Q})_{\text{tors}}$ such that

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}.$$

The integer r is called the *rank* of the elliptic curve and is denoted $\text{rank}_{\mathbb{Q}}(E)$, while $E(\mathbb{Q})_{\text{tors}}$ is called the *torsion subgroup* of E . The torsion subgroups of rational elliptic curves (up to isomorphism) are already completely understood and are classified by the following theorem:

Theorem 1.1 (Mazur [13]). *Let E/\mathbb{Q} be an elliptic curve. Then*

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4. \end{cases}$$

With the torsion subgroups of rational elliptic curves completely classified, we turn our attention to the ranks of rational elliptic curves. A first natural question to ask is:

Question 1.2. Let $S = \{\text{rank}_{\mathbb{Q}}(E) : E/\mathbb{Q} \text{ is an elliptic curve}\}$. Is the set S bounded above?

Despite much effort, this question remains unanswered and the mathematical community seems to be split on what to expect the answer to be. Recently in [17], Park, Poonen, Voight, and Wood have announced a heuristic that suggests that there are only finitely many elliptic curves of rank greater than 21, which would imply a positive answer to the above question. Their heuristic is based on modeling the ranks and Tate-Shafarevich groups simultaneously using alternating integer matrices.

In an attempt to better understand Question 1.2, many people have attempted to generate examples of elliptic curves with rank as large as possible. Much of the history of this endeavor has been catalogued by Dujella on his website [2] and the current record is an elliptic curve with rank at least 28 given by Elkies in [3]. Elkies was able to find 28 independent rational points of infinite order, showing that this curve has rank at least 28; with more advanced techniques, he showed that it has rank at most 32. This curve alone does

not contradict the heuristic presented in [17] since it permits finitely many elliptic curves with rank greater than 21.

As a refinement of this problem, one could ask if the ranks of elliptic curve over \mathbb{Q} with some added algebraic structure are unbounded. In particular, the ranks of elliptic curves with a given torsion structure have extensively studied. For example, the current rank record for an elliptic curve defined over \mathbb{Q} with torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is only 3. Rather than working on the well-studied question of the ranks of elliptic curves with prescribed torsion structures, we instead modify the question once again. Instead of requiring our elliptic curves to have a fixed torsion subgroup, we ask that they have an isogeny of fixed degree.

Definition 1.3. *An elliptic curve E/\mathbb{Q} is said to have a \mathbb{Q} -rational n -isogeny (or an isogeny of degree n) if E has a cyclic subgroup of order n defined over $\overline{\mathbb{Q}}$ that is stable under the component-wise action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

From this definition we can see that having an n -isogeny is a generalization of having a rational point of order n since any elliptic curve with a rational point of order n has a cyclic subgroup of order n that is stable under the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

With the techniques described below, we are able to prove the following theorem:

Theorem 1.4. *If n is a positive integer such that there is an elliptic curve over \mathbb{Q} with a rational n -isogeny, then there exists an elliptic curve over \mathbb{Q} with an n -isogeny and rank greater than or equal to 5.*

2. ELLIPTIC CURVES WITH ISOGENIES

By studying rational points on the classical modular curves $X_0(n)$, Mazur and Kenku were able to classify all of the integers n for which there is an elliptic curve defined over \mathbb{Q} with an n -isogeny.

Theorem 2.1. [13, 5, 6, 7, 8] *Let E/\mathbb{Q} be an elliptic curve with a rational n -isogeny. Then*

$$n \leq 19 \text{ or } n \in \{21, 25, 27, 37, 43, 67, 163\}.$$

Further, all of the \mathbb{Q} -rational points on the curves $X_0(n)$ have been fully classified, thus classifying (and parametrizing by j -invariant) all of the $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves with an isogeny of a given degree. This work was done by Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, and Ogg, among others. The results are spread vastly throughout the literature, but they have been collected into a single set of tables by Lozano-Robledo in [10, Tables 3 and 4].

From these tables, we see that the parametrizations come in two different forms depending on the genus of $X_0(n)$: when the genus of $X_0(n)$ is positive, there are finitely many $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves with n -isogenies, corresponding to a finite list of j -invariants; on the other hand, when the genus is zero, there are infinitely many $\overline{\mathbb{Q}}$ -isomorphism classes, with j -invariants parametrized as the image of a rational map. In our search for elliptic curves of moderate rank with n -isogenies, these two cases will require different approaches.

For some of the values of n given in Theorem 2.1, namely $2 \leq n \leq 10$ and $n = 12$, there exist elliptic curves with rational points of order n . Since an elliptic curve with a rational point of order n necessarily has an n -isogeny, the existing rank records for elliptic curves with prescribed torsion structures carry over to our search for curves of moderate rank with n -isogenies. Thus, although these curves with rational points of order n are not the only curves with n -isogenies for $2 \leq n \leq 10$ and $n = 12$, in order to avoid duplicating previous efforts we focus on the other values of n given in Theorem 2.1, for which no rank records have yet been established.

3. WHEN THE GENUS OF $X_0(n)$ IS POSITIVE.

To illustrate what can be done in this case, we start by giving the following definition:

Definition 3.1. Let C_1/\mathbb{Q} be a smooth projective curve. A twist of C_1/\mathbb{Q} is a smooth curve C_2/\mathbb{Q} such that C_2/\mathbb{Q} is isomorphic to C_1 over $\overline{\mathbb{Q}}$.

If the curves C_1 and C_2 above are elliptic curves, because the isomorphism between C_1 and C_2 is defined over $\overline{\mathbb{Q}}$ and *not* necessarily over \mathbb{Q} , it is possible that the set of rational points $C_1(\mathbb{Q})$ and $C_2(\mathbb{Q})$ are not isomorphic as groups. In particular, an isomorphism defined over $\overline{\mathbb{Q}}$ does not necessarily send rational points to rational points, and so it is possible that the ranks of C_1 and C_2 are different.

Definition 3.2. Let E/\mathbb{Q} be an elliptic curve given by Weierstrass equation $y^2 = x^3 + Ax + B$. For a non-zero rational $D \in \mathbb{Q}^\times$, the quadratic twist of E by D is the elliptic curve $E^{(D)}/\mathbb{Q}$ given by $y^2 = x^3 + AD^2x + BD^3$.

It is simple to check that if D is not a rational square, then E and $E^{(D)}$ are isomorphic over $\mathbb{Q}(\sqrt{D})$ and not isomorphic over \mathbb{Q} .

Proposition 3.3. Let E_1/\mathbb{Q} and E_2/\mathbb{Q} be elliptic curves that are isomorphic over $\overline{\mathbb{Q}}$. Further, suppose that $j(E_1) \neq 0$ or 1728. Then, either E_1 and E_2 are isomorphic over \mathbb{Q} , or E_2 is a quadratic twist of E_1 .

Proof. Let E_1 and E_2 be elliptic curves given by the Weierstrass equations $y^2 = x^3 + A_1x + B_1$ and $y^2 = x^3 + A_2x + B_2$ with $A_1, A_2, B_1, B_2 \in \mathbb{Z}$. Since $j(E_1) \neq 0$ or 1728 we know that A_1 and B_1 are both nonzero integers. Let $\varphi : E_1 \rightarrow E_2$ be an isomorphism defined over $\overline{\mathbb{Q}}$. By Proposition 3.1 in Chapter 3 of [22], we have that φ is given by $\varphi(x, y) = (u^2x, u^3y)$ for some $u \in \overline{\mathbb{Q}}$. Further, this means that $A_2 = u^4A_1$ and $B_2 = u^6B_1$. Since A_1, A_2, B_1 , and B_2 are all integers and A_2 and B_2 can't both be zero, it must be that u^2 is a nonzero rational number. Thus, either φ is defined over \mathbb{Q} or it is defined over a quadratic extension of \mathbb{Q} . \square

Remark 3.4. In the case where $j(E_1) = 0$ or 1728, E_2 may be a cubic or quartic twist of E_1 , rather than a quadratic one, since either $A_1 = A_2 = 0$ or $B_1 = B_2 = 0$. The curves in these two $\overline{\mathbb{Q}}$ -isomorphism classes have complex multiplication and do not appear in the list of curves that we are considering, so there is no need to consider these types of twists any further.

Proposition 3.5. Let E_1 and E_2 be elliptic curves defined over \mathbb{Q} such that E_2 is a quadratic twist of E_1 . Then, if E_1 has an n -isogeny, then E_2 also has an n -isogeny.

Proof. Again, let E_1 and E_2 be elliptic curves given by the Weierstrass equations $y^2 = x^3 + A_1x + B_1$ and $y^2 = x^3 + A_2x + B_2$ with $A_1, A_2, B_1, B_2 \in \mathbb{Z}$. Further, let $P = (x_0, y_0)$ be the generator of a Galois stable cyclic subgroup of order n . Since E_2 is a quadratic twist of E_1 , there is an isomorphism $\varphi : E_1 \rightarrow E_2$ given by $\varphi((x, y)) = (u^2x, u^3y)$ for some u with $u^2 \in \mathbb{Q}$. Because u^2 is rational, we know that $u = r\sqrt{D}$ for some squarefree integer D and some $r \in \mathbb{Q}$. We aim to show that $\langle \varphi(P) \rangle$ is Galois stable.

Take $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since $\langle P \rangle$ is Galois stable we know there exists $m_\sigma \in \mathbb{Z}$ such that $P^\sigma = m_\sigma P$. Further, by basic Galois theory we know that $\sigma(u) = \pm u$, so

$$\begin{aligned} \varphi(P)^\sigma &= (u^2x_0, u^3y_0)^\sigma = (\sigma(u^2x_0), \sigma(u^3y_0)) = (u^2\sigma(x_0), \pm u^3\sigma(y_0)) \\ &= \varphi(\pm P^\sigma) = \varphi(\pm m_\sigma P) = \pm m_\sigma \varphi(P). \end{aligned}$$

Thus $\langle \varphi(P) \rangle$ is Galois stable and of order n and E_2 has an n -isogeny. \square

3.1. Ranks of Quadratic Twists of Elliptic Curves. In the case when there are only finitely many $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves with an n -isogeny the idea is to search for quadratic twists of a fixed representative that have moderate rank. Much effort has been put into the study of the ranks of quadratic twists of elliptic curves and there are many open questions about the distribution of ranks in families of quadratic twists of elliptic curves. Of particular importance is the following conjecture due to Goldfeld.

Conjecture 3.6. *If E/\mathbb{Q} is an elliptic curve, then*

$$\lim_{X \rightarrow \infty} \frac{\sum_{|d| \leq X, d \text{ squarefree}} \text{rank}_{\mathbb{Q}}(E^{(d)})}{\#\{d \in \mathbb{Z} : |d| \leq X, d \text{ squarefree}\}} = \frac{1}{2}.$$

This conjecture together with the parity conjecture implies that for a fixed elliptic curve E the ranks of quadratic twists of E should be 0 half the time and 1 half the time. This makes finding twists of a fixed elliptic curve with rank greater than 1 a potentially difficult task and so the most obvious brute force method of checking the rank of every possible twist by a squarefree integer D with $|D|$ less than some bound is not a viable approach. The potentially highly non-trivial nature of the task of computing the rank of an elliptic curve, too, makes the brute force method intractable, so we need a more subtle approach: we want a heuristic that will allow us to determine (via a quicker computation) which twists are most likely to have higher rank than the others. We will then perform the full rank computations on these heuristically indicated curves.

3.2. The Method of Rogers. To do this, we use the method outlined in [18], where Rogers searches for twists of moderate rank of the congruent number elliptic curve given by $y^2 = x^3 - x$. The method begins by letting E/\mathbb{Q} be an elliptic curve given by Weierstrass equation $y^2 = f(x)$ and then writing the elliptic curve $E^{(D)}$ in the nonstandard form $Dy^2 = f(x)$. With $E^{(D)}$ written this way, Gouvêa and Mazur observed in [4] that if $r \in \mathbb{Q}$ and D_r is the unique square-free integer such that $D_r \equiv f(r) \pmod{(\mathbb{Q}^\times)^2}$, then the curve $E^{(D_r)}$ has a rational point whose x -coordinate equal to r .

The idea, suggested to Rogers by Rubin and Silverberg, is to fix a height bound H and see which integers occur most often as D_r for some $r \in \mathbb{Q}$ with height less than H . The more times a given integer D occurs, the more points of low (naive) height are present on the curve $E^{(D)}$. The twists of E that have many such points should tend to have higher rank and so these twists are the ones whose rank it is most worthwhile to compute. While this is not always completely correct,¹ it does give us an efficient way to identify promising candidates in our search for twists of high rank.

In the table below, we give the degree n of the isogeny each curve has, the j -invariant as well as the a -invariants that define the curve with smallest conductor in the $\overline{\mathbb{Q}}$ -isomorphism class, the upper bound H we used for the heights of the rational numbers, and the twists of maximal rank that we found. For each degree n , the highest rank found for a curve with an n -isogeny is highlighted in boldface type. In each case, we first performed a search using Rogers's method in SAGE, then used Magma to compute the Selmer ranks of the top 100 most frequently appearing twists, and finally computed the actual rank and generators of the most promising curves.

In almost all cases, we were able to use $H = 10^4$, but in two cases the size of the coefficients of the elliptic curves with smallest conductor in the $\overline{\mathbb{Q}}$ -isomorphism class prevented us from searching all the way out to $H = 10^4$ in a reasonable amount of time and we were instead forced to take $H = 5 \cdot 10^3$ or even $H = 10^3$. The difficulty here arises from the fact that the task of computing the squarefree part $D_{f(x)}$ of $f(x)$ is equivalent in complexity to the task of factoring $f(x)$. Indeed, for $n = 163$ this search did not provide any elliptic curves of rank greater than that of the original (i.e., “untwisted”) curve. We use a new method to deal with this particular case.

3.3. A New Method for Finding Twists of Moderate Rank. Let E/\mathbb{Q} be an elliptic curve. If p is a prime of good reduction for E , then let $N_p = \#E(\mathbb{F}_p)$ and $a_p = p + 1 - N_p$; otherwise, let

$$a_p = \begin{cases} 1 & \text{if } E \text{ has split multiplicative reduction at } p, \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p, \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

¹An elliptic curve of rank 1 might have many points of small naive height, while an elliptic curve of higher rank might not have any of the same height.

| j | n | a -invariants of E | H | D | $\text{rank}_{\mathbb{Q}}(E^{(D)})$ |
|---|-----|---|----------------|--------------|-------------------------------------|
| $-11 \cdot 131^3$ | 11 | $[1, 1, 1, -30, -76]$ | 10^4 | -97966 | 4 |
| -2^{15} | 11 | $[0, 0, 0, -9504, 365904]$ | 10^4 | -64259 | 4 |
| -11^2 | 11 | $[1, 1, 0, -2, -7]$ | 10^4 | -1472782 | 5 |
| $-3^3 \cdot 5^3$ | 14 | $[0, 0, 0, -2835, -71442]$ | 10^4 | -883554 | 4 |
| $3^3 \cdot 5^3 \cdot 17^3$ | 14 | $[0, 0, 0, -595, -5586]$ | 10^4 | -4541835 | 5 |
| $-5^2/2$ | 15 | $[0, 0, 0, -675, -79650]$ | 10^4 | -1734994 | 5 |
| $-5^2 \cdot 241^3/2^3$ | 15 | $[0, 0, 0, -162675, -25254450]$ | 10^4 | -3163927 | 5 |
| $-5 \cdot 29^3/2^5$ | 15 | $[0, 0, 0, -3915, 113670]$ | 10^4 | 1951555 | 4 |
| $5 \cdot 211^3/2^{15}$ | 15 | $[0, 0, 0, 28485, -838890]$ | 10^4 | -39947 | 4 |
| $-17^2 \cdot 101^3/2$ | 17 | $[1, 0, 1, -3041, 64278]$ | 10^4 | 703 | 5 |
| $-17 \cdot 373^3/2^{17}$ | 17 | $[1, 0, 1, -3041, 64278]$ | 10^4 | 11951 | 5 |
| $-2^{15} \cdot 3^3$ | 19 | $[0, 0, 1, -38, 90]$ | 10^4 | 182766 | 5 |
| $-3^2 \cdot 5^6/2^3$ | 21 | $[0, 0, 0, -75, 262]$ | 10^4 | 5107035 | 5 |
| $3^3 \cdot 5^3/2$ | 21 | $[0, 0, 0, 45, -18]$ | 10^4 | -2606345 | 5 |
| $-3^2 \cdot 5^3 \cdot 101^3/2^{21}$ | 21 | $[0, 0, 0, -122715, -33611274]$ | 10^4 | -531894503 | 5 |
| $-3^3 \cdot 5^3 \cdot 383^3/2^7$ | 21 | $[0, 0, 0, -17235, 870894]$ | 10^4 | 4094 | 4 |
| $-2^{15} \cdot 3 \cdot 5^3$ | 27 | $[0, 0, 0, -480, 4048]$ | 10^4 | 1058402 | 5 |
| $-7 \cdot 11^3$ | 37 | $[1, 1, 1, -8, 6]$ | 10^4 | 21880474 | 5 |
| $-7 \cdot 137^3 \cdot 2083^3$ | 37 | $[0, 0, 0, -269675595, -1704553285050]$ | $5 \cdot 10^3$ | -3791 | 4 |
| $-2^{18} \cdot 3^3 \cdot 5^3$ | 43 | $[0, 0, 0, -13760, 621264]$ | 10^4 | 18618 | 5 |
| $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ | 67 | $[0, 0, 0, -117920, 15585808]$ | 10^4 | 37630 | 5 |
| $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ | 163 | $[0, 0, 0, -34790720, 78984748304]$ | 10^3 | 1 | 1 |

TABLE 1. Twists in the positive genus case

A consequence of the Sato-Tate conjecture is that the proportion of primes for which a_p is positive is equal to the proportion of primes for which a_p is negative. With this in mind, Mazur in [14] considers the quantity

$$D_E(t) = \sum_{p \leq t} \text{sgn}(a_p).$$

Given the Sato-Tate conjecture, one might expect that the values of $D_E(t)$ would be close to zero for large values of t , yet Mazur found experimentally that for curves of higher rank, $D_E(t)$ is more biased toward being negative. To illustrate this phenomenon, Mazur plots $(t, D_E(t))$ for $t \leq 10^6$ for the elliptic curves with Cremona labels 11A, 37A, 389A, and 5077A. These curves have rank 0, 1, 2, and 3 respectively, and Mazur observes that the larger the rank of the curve, the larger the bias is for $D_E(t)$ to be negative.

One can make intuitive sense of this phenomenon with the following two observations: firstly, there should in general be about $p + 1$ points on an elliptic curve E/\mathbb{F}_p , and secondly, a curve with more rational points ought to have more points, on average, when reduced modulo a prime p . Thus the sign of a_p tells us exactly when the reduction curve has more or fewer points than the expected average, and so the more frequently the number of points modulo p exceeds the naive expectation of $p + 1$, the more frequently $\text{sgn}(a_p)$ will be negative and the more $D_E(t)$ will trend in the negative direction.

Looking at figures 2.2 – 2.5 in [14], we see that while $D_E(10^6)$ is a good indicator of the rank of E , a better indicator for these curves is $\min\{D_E(t) : t \leq 10^6\}$. Thus, if we wanted to use this to find twists of moderate rank, we could compute $\min\{D_{E'}(t) : t \leq 10^6\}$ for many twists E' of E and use the resulting values to pick twists on which to perform the full rank computation.

Remark 3.7. This method is computationally simpler than the method described above since there is no factoring necessary and counting the points on an elliptic curve over a finite field can be done very efficiently. Furthermore, since at each step of the computation we are at most incrementing or decrementing the running total, we are able to compute the values in question quickly and without requiring much memory.

On the other hand, this method places an explicit bound on the magnitudes of the squarefree integers by which we are twisting the original curve. In the particular case in which we used it, for example, we only considered twists by integers up to 10^6 . Rogers’s method, meanwhile, sets a bound on the heights of the rationals x for which we compute the squarefree parts $D_{f(x)}$ of $f(x)$; while this imposes an implicit bound on the size of the twists considered, it is a much looser one, and twists by squarefree integers of much greater magnitude occur. For instance, note that in our search, in which we considered rationals x of height up to 10^4 , one of the curves of rank 5 with a 21-isogeny was given by twisting by -531894503 . This explicit restriction is, at least conjecturally, a real disadvantage: since the rank of an elliptic curve E with conductor N_E is conjectured to be bounded by $C \frac{\log N_E}{\log \log N_E}$ for some constant C ,² and since the conductor of $E^{(D)}$ is essentially $D^2 \cdot N_E$, we want to allow twists by large integers in our search for twists of large rank.

We take E to be the minimal twist of the single $\overline{\mathbb{Q}}$ -isomorphism class of elliptic curves with 163-isogenies. We compute $\min\{D_{E^{(D)}}(t) : t \leq 10^5\}$ for every squarefree D with $|D| \leq 10^6$ and then compute the ranks of the 100 most promising curves, producing a curve of rank 5, namely $E^{(D)}$ with $D = 376085$.

| j | n | a -invariants of E | D | $\text{rank}_{\mathbb{Q}}(E^{(D)})$ |
|---|-----|-------------------------------------|--------|-------------------------------------|
| $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ | 163 | $[0, 0, 0, -34790720, 78984748304]$ | 376085 | 5 |

TABLE 2. A new method for the case $n = 163$

4. WHEN THE GENUS OF $X_0(n)$ IS ZERO.

When the modular curve $X_0(n)$ has genus zero, we have that $X_0(n)(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$ and that there are infinitely many rational points corresponding to $\overline{\mathbb{Q}}$ -isomorphism classes of rational elliptic curves with an n -isogeny. In this case, the j -invariants of these elliptic curves are given as the image of a rational map $j_n : X_0(n) \simeq \mathbb{P}^1 \rightarrow \mathbb{Q}$. For example,

$$j_{13}(h) = \frac{(h^2 + 5h + 13)(h^4 + 7h^3 + 20h^2 + 19h + 1)^3}{h}.$$

Therefore we need an efficient way to determine for what values of $h \in \mathbb{Q}$ the minimal twist of the $\overline{\mathbb{Q}}$ -isomorphism class of curves with j -invariant $j_n(h)$ is *likely* to have large rank. To do this we will use a heuristic attributed to Nagao which concerns the L -function of an elliptic curve.

²For more details, see [23, Conjecture 10.5].

4.1. L -functions of Elliptic Curves. Throughout this section let E/\mathbb{Q} be an elliptic curve. If p is a prime, we define N_p and a_p as above.

Definition 4.1. For any prime p , the local factor at p of the L -series is defined to be

$$L_p(T) = \begin{cases} 1 - a_p T + pT^2, & \text{if } E \text{ has good reduction at } p, \\ 1 - T, & \text{if } E \text{ has split multiplicative reduction at } p, \\ 1 + T, & \text{if } E \text{ has non-split multiplicative reduction at } p, \\ 1, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

The L -function of the elliptic curve E is defined to be

$$L(E, s) = \prod_{p \geq 2} \frac{1}{L_p(p^{-s})},$$

where the product is taken over all primes p .

The importance of L -functions derives principally from the following conjecture, which connects the algebraic structure of an elliptic curve with the behavior of its associated L -function, giving an analytic method for computing the rank of the curve.

Conjecture 4.2 (Birch and Swinnerton-Dyer). Let E be an elliptic curve over \mathbb{Q} , and let $L(E, s)$ be the L -function of E . Then $L(E, s)$ has a zero at $s = 1$ of order equal to $\text{rank}_{\mathbb{Q}}(E)$.

In fact, the Birch and Swinnerton-Dyer conjecture says more than what is stated above. It also gives a formula for the residue of $L(E, s)$ at $s = 1$ in terms of various invariants of E , but for our purposes this weaker version is sufficient. For more information, the reader is encouraged to see [19] or [11].

Assuming this conjecture, we can write $L(E, s) = (s - 1)^{R_E} \cdot g(E, s)$, where $g(E, s)$ is some function such that $g(E, 1) \neq 0$ and $R_E = \text{rank}_{\mathbb{Q}}(E)$. Computing the log derivative of $L(E, s)$ yields

$$\frac{L'(E, s)}{L(E, s)} = R_E \cdot \frac{1}{s - 1} + h(E, s)$$

where $h(E, s) = g'(E, s)/g(E, s)$ is analytic close to $s = 1$. Therefore,

$$\lim_{s \rightarrow 1} \frac{L'(E, s)}{L(E, s)} = R_E \lim_{s \rightarrow 1} \frac{1}{s - 1} + h(1),$$

and the rank of E can be estimated using the rate at which the limit goes to infinity.

The problem with this estimation is that computing the L -function of an elliptic curve is time consuming if it is possible at all. So Nagao defined the following finite product,

$$L_N(E, s) = \prod_{p \leq N} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

as an approximation to the L -function $L(E, s)$.

The products $L(E, s)$ and $L_N(E, s)$ have two main differences. The most apparent discrepancy is that $L_N(E, s)$ is truncated to be a finite product rather than an infinite one. The other difference is that $L_N(E, s)$ ignores the deviation between the local factors of primes of good and bad reduction. Treating every prime as if it were a prime of good reduction makes computing the truncated L -function for *many* different elliptic curves easier while only changing a finite number of terms in each product. Thus, $L(E, s)$ and $\lim_{N \rightarrow \infty} L_N(E, s)$ should still be closely related.

Next, taking the logarithm of $L_N(E, s)$, defining the resulting sum to be $f_N(E, s)$, and taking the derivative shows that

$$f'_N(E, s) = - \sum_{p \leq N} \frac{a_p p^{-s} - 2p^{1-2s}}{1 - a_p p^{-s} + p^{1-2s}} \log p.$$

If we expect $L(E, s)$ and $\lim_{N \rightarrow \infty} L_N(E, s)$ to be closely related, we should also expect $\lim_{N \rightarrow \infty} f'_N(E, s)$ to be a good approximation to the log derivative of $L(E, s)$, and so

$$\lim_{s \rightarrow 1} \frac{L'(E, s)}{L(E, s)} \approx \lim_{s \rightarrow 1} \lim_{N \rightarrow \infty} f'_N(E, s).$$

Finally, since our goal is to arrive at a rough heuristic, we switch the limits on the right-hand side without justification to get

$$\lim_{s \rightarrow 1} \frac{L'(E, s)}{L(E, s)} \approx \lim_{N \rightarrow \infty} f'_N(E, 1) = \lim_{N \rightarrow \infty} - \sum_{p \leq N} \frac{a_p p^{-1} - 2p^{-1}}{1 - a_p p^{-1} + p^{-1}} \log p = \lim_{N \rightarrow \infty} \sum_{p \geq N} \frac{2 - a_p}{N_p} \log(p).$$

Therefore, if we let

$$S(E, N) = f_N(E, 1) = \sum_{p \geq N} \frac{2 - a_p}{N_p} \log(p),$$

we should be able to use $S(E, N)$ for some sufficiently large N to distinguish between elliptic curves of large and small rank. That is to say, when $S(E, N)$ is relatively large, we have reason to suspect that E itself has relatively large rank.

Remark 4.3. The heuristic we use here was first used by Nagao in [16] where he used this heuristic and a construction of Mestre to generate an elliptic curve of rank greater than or equal to 20. It was then used again by Watkins, Donnelly, Elkies, Fisher, Granville, and Rogers as described in [24]. One could form many slightly different sums over small primes that all ought to correlate with the rank of a fixed elliptic curve. For a more detailed discussion of these variations and their respective advantages and disadvantages, see [24, §5].

For each $r \in \mathbb{Q}$ with height less than some bound H , we let $E_{j_n(r)}$ be the minimal model of the elliptic curve with j -invariant $j_n(r)$ and use SAGE to compute $S(E_{j_n(r)}, N)$ for some fixed “large” N . Then we use Magma to compute the Selmer ranks and actual ranks of the elliptic curves E for which $S(E, N)$ is largest.

For $n = 13$ and 16 we let $N = 10^4$ and $H = 200$ to get the following table of data.

| n | r | a -invariants | $\text{rank}_{\mathbb{Q}}(E_{j_n(r)})$ |
|-----|---------|--|--|
| 13 | 101/60 | [1, 0, 1, -288446980524976098, 59625981683441978523832756] | 6 |
| 13 | -113/20 | [0, 0, 0, -452597990381667, 3706144386347090080926] | 5 |
| 13 | 9/8 | [1, 1, 1, -8657699123, 309987918855281] | 4 |
| 16 | 187/40 | [1, 1, 1, -30111109596200490, 201112119279475857520645] | 4 |
| 16 | 77/80 | [1, 1, 1, -105028852953910, 11925868172151407627315] | 3 |
| 16 | 167/114 | [1, 0, 0, 21676796948537980, 1144823745894014005574160] | 2 |

TABLE 3. Searching in the genus zero case with the Nagao heuristic

However, a problem arises when we try and use this method for $n = 18$ and 25 . While it is possible to use the heuristic above to compute the elliptic curves that *should* have high rank, the conductors of these curves are so large that Magma is unable to compute their Selmer rank, let alone actual rank, in a reasonable amount of time. In order to find elliptic curves of moderate rank with isogenies of degree 18 or 25, we need a different approach, so we revert to the method of Rogers outlined in Section 3. The idea is to use [9] to find the elliptic curves with minimal conductor among those with an 18-isogeny and among those with a 25-isogeny. We then use Rogers’s method to look for twists of these curves that have moderate rank. In fact, we also applied this method to the cases of $n = 13$ and 16 to see how the two methods compare. Below we give a table of the results obtained from these searches.

| j | n | a -invariants of E | H | D | $\text{rank}_{\mathbb{Q}}(E^{(D)})$ |
|---------------------------------|-----|------------------------|--------|-------------|-------------------------------------|
| $-1 \cdot 2^{12} \cdot 7/3$ | 13 | $[0, -1, 1, -2, -1]$ | 10^4 | 70557 | 4 |
| $-1 \cdot 3^3 \cdot 7/2$ | 13 | $[1, -1, 0, -2, 6]$ | 10^4 | -1049 | 4 |
| $-1/15$ | 16 | $[1, 1, 1, 0, 0]$ | 10^4 | -1625560485 | 6 |
| $5281^3/(3^4 \cdot 5 \cdot 13)$ | 16 | $[1, 0, 0, -110, 435]$ | 10^4 | 59243810 | 7 |
| $-1 \cdot 5^6/(2^2 \cdot 7)$ | 18 | $[1, 0, 1, -1, 0]$ | 10^4 | -10533149 | 6 |
| $-1 \cdot 2^1 2/11$ | 25 | $[0, -1, 1, 0, 0]$ | 10^4 | -203145767 | 6 |
| $-1 \cdot 269^3/(2 \cdot 11)$ | 25 | $[1, 1, 1, -28, -69]$ | 10^4 | 4817182 | 6 |

TABLE 4. Twists in the genus zero case

For each value of n we considered—that is, for each n appearing in Theorem 2.1 besides those for which there exist elliptic curves with rational points of order n —our searches produced an elliptic curve of rank at least 5 with an n -isogeny. We would like to extend this baseline minimum of rank 5 to all possible isogeny degrees, so we now turn our attention briefly to the others, namely $2 \leq n \leq 10$ and $n = 12$. For $2 \leq n \leq 8$, there are known examples of elliptic curves of rank at least 5 that have torsion group isomorphic to $\mathbb{Z}/n\mathbb{Z}$ (see [2]) and thus have an n -isogeny. This leaves the three cases of $n = 9$, $n = 10$ and $n = 12$. In each case, the highest known rank of a curve with torsion group isomorphic to $\mathbb{Z}/n\mathbb{Z}$ is only 4. However, the curve of rank 6 with an 18-isogeny that our search found also has a 9-isogeny,³ so we have a curve of rank at least 5 with a 9-isogeny.

For $n = 10$ and $n = 12$, we conducted searches using the method of Rogers, producing the following data.

| j | n | a -invariants of E | H | D | $\text{rank}_{\mathbb{Q}}(E^{(D)})$ |
|---|-----|------------------------------|--------|------------|-------------------------------------|
| $179^3 \cdot 2699^3/(2^2 \cdot 3 \cdot 11^5)$ | 10 | $[1, 0, 0, -10065, -389499]$ | 10^4 | -802314609 | 5 |
| $-11^3 \cdot 59^3/(2^1 2 \cdot 3 \cdot 5^3)$ | 12 | $[1, 0, 1, -14, -64]$ | 10^4 | -148243395 | 5 |

TABLE 5. Twists for $n = 10$ and 12

The data in Tables 1, 2, 3, 4, and 5, together with the rank records recorded by Dujella at [2], justify the following result.

Theorem 4.4. *If n is a positive integer appearing in Theorem 2.1, then there exists an elliptic curve with an n -isogeny and rank greater than or equal to 5.*

5. ACKNOWLEDGEMENTS

The authors would like to thank Filip Najman for suggesting this project and Álvaro Lozano-Robledo and Steven J. Miller for helpful conversations throughout the process as well as the referee and editors for their useful comments and a quick editorial process. Both authors would also like to thank the Amherst College Department of Mathematics and Statistics for its support of the undergraduate thesis project during which this work was carried out.

³To see this, let E be the curve in question and take P to be a generator of the Galois stable cyclic subgroup $G \subseteq E(\overline{\mathbb{Q}})$ of order 18, and consider the subgroup generated by $2P$.

REFERENCES

- [1] H. Daniels and H. Goodwillie, Magma/SAGE scripts and data related to *On the ranks of elliptic curves with isogenies*, available at https://www3.amherst.edu/~hdaniels/rank_data.
- [2] A. Dujella, “History of Elliptic Curves Rank Records”, available at <https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html>. [1](#), [4.1](#), [4.1](#)
- [3] N. Elkies, \mathbb{Z}^{28} in $E(\mathbb{Q})$, Number Theory Listserver, May 2006. [1](#)
- [4] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4**:1 (1991), 1–23. [3.2](#)
- [5] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23. [2.1](#)
- [6] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20. [2.1](#)
- [7] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244. [2.1](#)
- [8] M. A. Kenku, *The modular curve $X_0(125)$, $X_1(25)$ and $X_1(49)$* , J. London Math. Soc. (2) **23** (1981), 415–427. [2.1](#)
- [9] LMFDB Collaboration, *The L-functions and modular forms database*, available at <http://www.lmfdb.org>. [4.1](#)
- [10] Á. Lozano-Robledo, *On the field of definition of p -torsion points on elliptic curves over the rationals*, Mathematische Annalen, Vol 357, Issue 1 (2013), 279–305. [2](#)
- [11] Á. Lozano-Robledo, *Elliptic Curves, Modular Forms, and Their L-functions*, American Mathematical Society, Providence, Rhode Island, 2010. [4.1](#)
- [12] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265.
- [13] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162. [1.1](#), [2.1](#)
- [14] B. Mazur, *Finding meanings and error terms*, Bull. Amer. Math. Soc. **45** (2008), no. 2, 185–228. [3.3](#)
- [15] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Philos. Soc. **21** (1922), 179–192. [1](#)
- [16] K. Nagao, *An Example of Elliptic Curve over \mathbb{Q} with Rank ≥ 20* , Proc. Japan Acad., **69** (1993), 291–293. [4.3](#)
- [17] J. Park, B. Poonen, J. Voight, and M. Wood *A heuristic for boundedness of ranks of elliptic curves*, available at <http://arxiv.org/abs/1602.01431>. [1](#)
- [18] N. F. Rogers, *Rank computations for the congruent number elliptic curves*, Experiment. Math. **9**, no. 4 (2000), 591–594. [3.2](#)
- [19] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. **39** (2002), 455–474. [4.1](#)
- [20] Sage Mathematics Software (Version 6.10.0), The Sage Developers, 2015, <http://www.sagemath.org>.
- [21] A. Silverberg, *The distribution of ranks in families of quadratic twists of elliptic curves*, Ranks of elliptic curves and random matrix theory, 171–176, London Math. Soc. Lecture Note Ser., 341, Cambridge Univ. Press, Cambridge, 2007.
- [22] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 2nd Edition, New York, 2009. [3](#)
- [23] D. Ulmer, *Elliptic curves with large rank over function fields*, Annals of Mathematics, **155** (2002), 295 – 315 [2](#)
- [24] M. Watkins, S. Donnelly, N. D. Elkies, T. Fisher, A. Granville, and N. F. Rogers, *Ranks of quadratic twists of elliptic curves*, Numéro consacré au trimestre “Méthodes arithmétiques et applications”, automne 2013, 63–98, Publ. Math. Besançon Algèbre Théorie Nr., 2014/2, Presses Univ. Franche-Comté, Besançon, 2015. [4.3](#)
- [25] A. Weil, *L’arithmétique sur les courbes algébriques*, Acta Math. **52** (1929) 281–315. [1](#)

DEPARTMENT OF MATHEMATICS AND STATISTICS, AMHERST COLLEGE, AMHERST, MA 01002, USA
E-mail address: hdaniels@amherst.edu
URL: <http://www3.amherst.edu/~hdaniels/>

DEPARTMENT OF MATHEMATICS AND STATISTICS, AMHERST COLLEGE, AMHERST, MA 01002, USA
E-mail address: hannah.goodwillie@gmail.com